vipax

symantec VIP Access emulation eXec

概要

最近のネットバンキング等では電子証明書方式から、30 秒毎に生成される一定の 6 文字の数字を使い捨てパスワード(ワンタイムパス)として入力させるハードないしソフトトークン方式に移行ないしこれを併用するする方向にあり、特にソフトトークンでは Symantec 社の「VIP Access」が多く使われるようになってきています。

本ソフトはこの「VIP Access」のワンタイムパスをエミュレーション生成するものです。

トークンとはこのワンタイムパスを生成するデバイスで、一個の独立したハードで生成する方式(ハードトークン)と、PC 上のソフトから生成する方式(ソフトトークン)が存在します。

ネットバンキング等でのトークン方式の問題点は、電子証明書方式の場合と同様、そのトークンの ID がバンキングサーバー側に登録され、そのトークンでしか有効なワンタイムパスを生成できないことです。これはセキュリティ上の要請ですが、そのトークンが壊れた場合は、面倒な文書による店頭再申請となるわけです。ハードトークンであれば簡単には壊れないでしょうが、ソフトトークンの場合はその PC が壊れる場合に限らず、機種入替えはもとより OS 再インストールでもそのソフトトークンは無効になるのです。

ところでハード及びソフトトークンは、どちらも世界標準のアルゴリズムに基づき一定のシークレットコードと現在の時間からワンタイムパスを生成します。よってこのシークレットコードが判明すればワンタイムパスも判明するのですが、ハードトークンではこのシークレットコードがハードの中に対タンパ状態で存在するため原理的にはこれを探知することができません。ところがソフトトークンの場合はこれが可能です。

本ソフトは、ソフトトークンである「VIP Access」のシークレットコードを探知し、ワンタイムパスをエミュレーション生成します。そしてそれはどの PC からでも可能です。よってトークンを登録した PC が動かなくなっても面倒な店頭再申請は不要です。

但し「VIP Access」はその PC のハード状態によってワンタイムパスの生成方式が変わります。
最近の PC(マザーボード)で一般的になりつつある「Intel® Management Engine Interface(Intel MEI)」と「Intel® Identity Protection Technology (Intel® IPT)」が存在する場合、「VIP Access」はこの Intel のハードテクノロジを使い、ソフトトークンでありながら実態はハードトークンと同等になり、結果、本ソフトはそのシークレットコードを探知できなくなります。
しかしながらこの問題点は、本ソフト内より一時的に「Intel MEI」を停止することで解決できます(詳細後述)。

動作確認環境

Windows 環境でのみ動作します。以下の OS 環境であればそれ以上の動作要件はありません。
　対応プラットフォーム x86(IA-32)と x64　(その他のプラットフォームには対応していません)
　x86 環境
　　WindowsXP-SP3　Windows2003-R2-SP2　Windows2008-R1-SP2
　　Windows7　Windows7-SP1　Windows8　Windows8.1
　x64 環境
　　Windows2008-R2-SP1　Windows7　Windows7-SP1　Windows8　Windows2012　Windows8.1　Windows10

これ以外の OS 環境では動作検証されていません。x64 環境で x86 版は(WOW64)動作に制限があります。

同梱ファイル

vipax本体　vipax32.exe（x86用実行ファイル）　vipax64.exe（x64用実行ファイル）
その他説明書(本ファイル。尚、本ファイルを上記実行ファイルと同じディレクトリに置いてください。)

インストール

インストール作業は不要です。実行ファイルをエクスプローラー等から直接起動してください。
尚、バージョンアップ時には本ソフトを起動後一旦「完全終了」ボタンで終了してから再起動してください。

アンインストール

本ソフトは起動するとシステムのいくつかのレジストリを使用する他、テンポラリフォルダでいくつかのファイルを生成します。しかし「完全終了」ボタンを押して終了することでこれらを削除し導入前の環境に戻せます。
すなわちアンインストール作業は不要です。
「完全終了」ボタンによる終了は、原則本ソフトによるシステムへの残存物を全て削除しますが、
本ソフトが試用制限を設けている関係上、試用関係情報のみ例外としてシステムに残存させてもらっています。
尚、本ソフトの使用レジストリは以下で画面位置等を記録しています。
　HKEY_LOCAL_MACHINE¥SOFTWARE¥vipax　KEY_LOCAL_MACHINE¥SOFTWARE¥vipax_regist

シェアウェア・試用・試用中の制限について

本ソフトは起動回数「10 回まで」、インストール後「7 日間」試用することができる「シェアウェア」です。
その間で、お使いの環境での動作確認を行っていただき、継続使用する場合はご購入ください。
試用期間中は機能制限はありません。試用期間経過後はバックアップとワンタイムパス表示ができなくなります。

金額・支払方法について

ソフト本体価格(消費税別)5,600 円です。支払方法は原則「ベクタシェアレジ」のみとなります。
ベクタシェアレジがなんらかの事情で利用できない方は下記メールアドレスへ連絡ください。
個別に折返し、銀行振込による方法をご連絡します。

連絡先

作者への連絡先は下記のとおりです。
ハンドル 丸太
メールアドレス　qqcr2rd9k@arion.ocn.ne.jp

その他注意事項

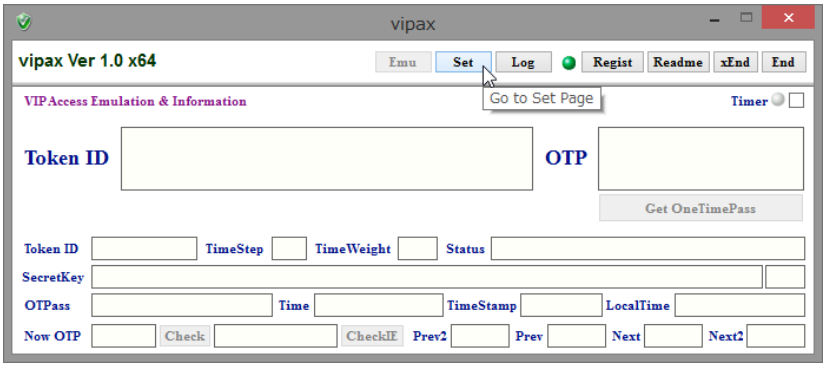
① ドライブを暗号化するソフトで「システムドライブ」全体を暗号化してある場合「vipax」は試用回数及び期間の計測を誤り、初回起動時いきなり試用回数または期限超過になります。そのような環境では「試用」できないことをご了承ください。
② システムに、物理ハードディスクが最低 1 台接続されている必要があります。具体的には Windows システム上に「¥¥.¥PhysicalDrive0」のシンボリックリンクが存在している必要があります。

簡単使用方法

ここでは仮に Windows8.1x64 環境の例で説明します（他の環境では多少の違いがありますが同様です）。

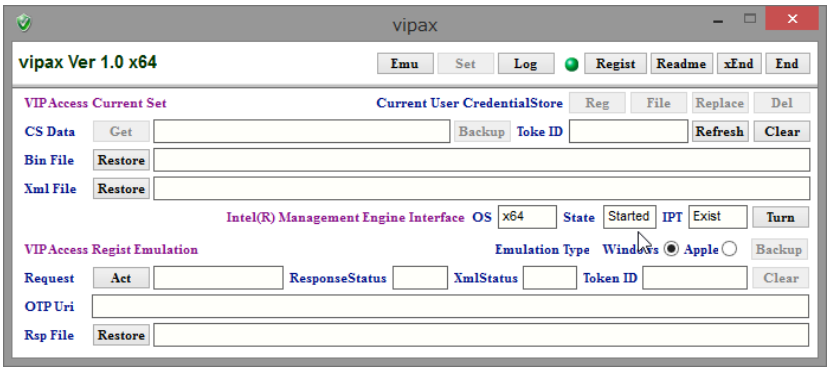
起動

本ソフトを起動すると以下のような画面になるので「Set」ボタンを押してください。

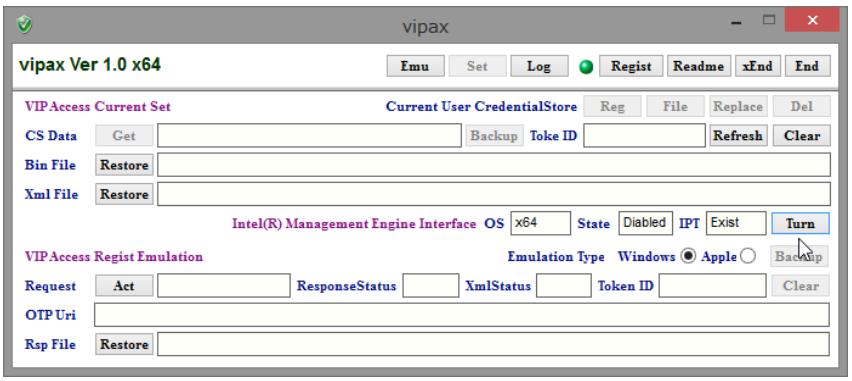


初期処理

次のような画面になります。



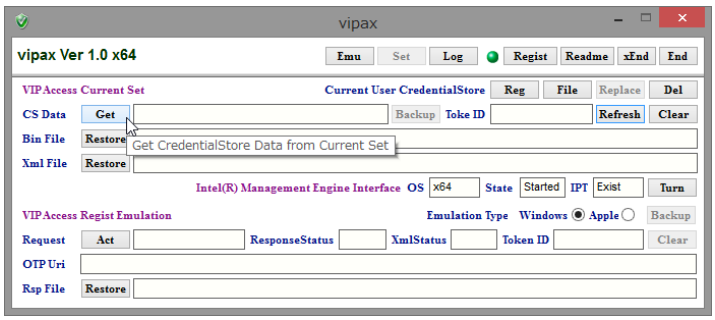
「Intel(R) Management Engine Interface」の「State」の部分に着目してください。
「State」が「Started」で「IPT」が「Exist」の場合「Intel IPT」が稼働している状態で、
このままでは完全エミュレーションができません。
右の「Turn」ボタンを押して一時的に「Intel MEI」を無効化してください。



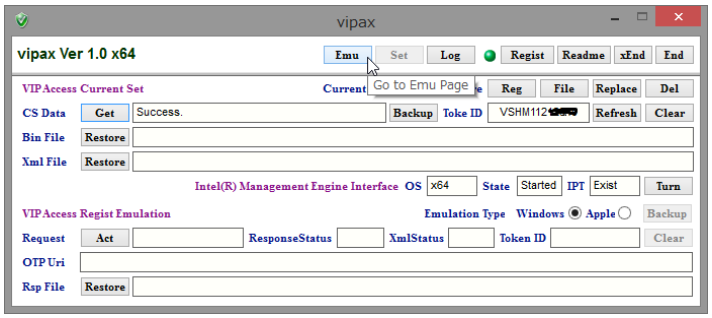
また「Turn」ボタンを押せば「Intel MEI」は有効化します。
尚、この「Turn」ボタンは「WOW64」環境では機能しません。
「Intel MEI」の「State」が「Started」でも「IPT」が「(non)」と表示される環境ではこれらは問題になりません。
以降しばらく「Intel IPT」が稼働している環境を前提に話を進めますが、該当しない方は読み飛ばしてください。

「INTEL IPT」が稼働している状態で既に「VIP ACCESS」を起動している場合

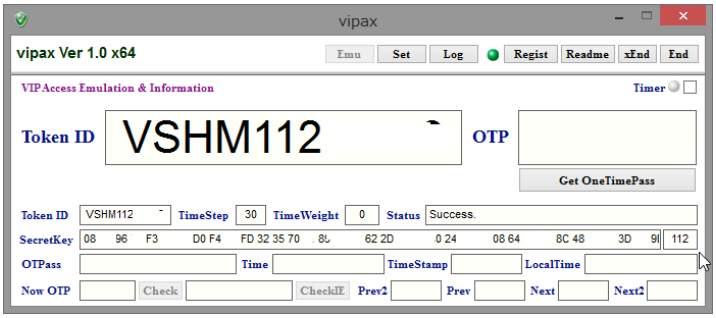
既に「VIP Access」を「Intel IPT」稼働下の PC で起動してしまっている場合、次のような画面になります。
「Get」ボタンが有効化していますのでこれを押してください。



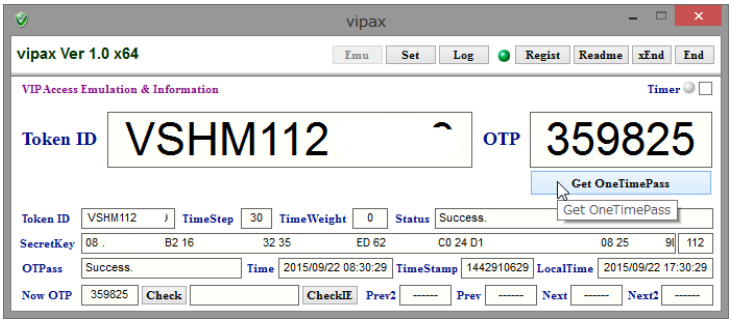
現在の「VIP Access」のデータが読込まれ、解析が完了し以下のような画面になります。
ここで「Success」と表示されない場合(エラー時)は、現在の「VIP Access」のデータ読込み失敗を示します。
「Emu」ボタンを押して「Emu ページ」に行ってください。



このような画面になります。「SecretKey」の右端が「112」と表示されています。これが「20」でない場合、
既に「VIP Access」が「Intel IPT」の稼働下で動いていることを示します。



「Get OneTimePass」ボタンを押してみてください。



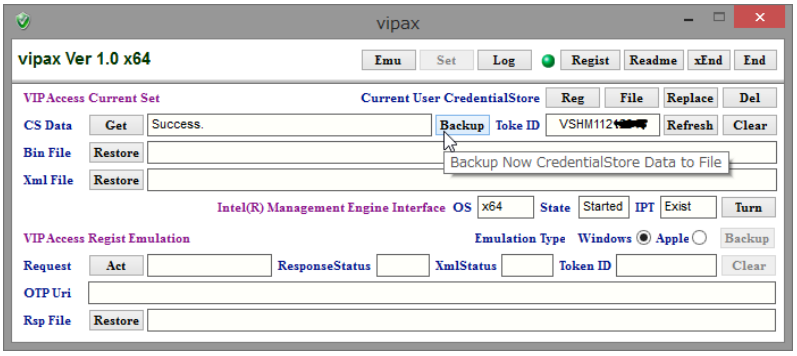
一応本ソフトは「Intel IPT」稼働下の現在のワンタイムパスを「Intel IPT」のモジュールを使い表示できます。
しかし、この状態では他の PC に移行してそれをエミュレートすることができません。
また、たった今現在のワンタイムパスが判明するだけで、前回(Prev)や次回(Next)のワンタイムパスはわかりません。

他の PC でもエミュレーションしたい場合は結論的に、現在の「VIP Access」の(CredentialStore)データを一旦削除する必要があります。とはいえ、それはバックアップしておくことで後で復元できます。
ただ、そのバックアップはその PC でしか使えません。

注意！

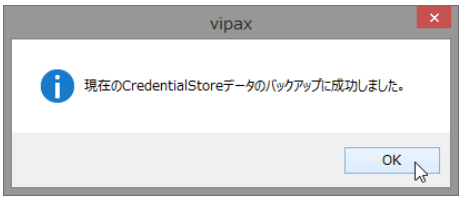
ここで削除する(CredentialStore)データはネットバンキング等のサーバーに既に登録されています。
これから、それを削除し新たな(CredentialStore)データを作成し使うということになりますので、ネットバンキング等のサーバー側にそのことを伝達しなければなりません。
すなわちネットバンキングでは「ワンタイムパスの(Token ID の)登録解除と再登録」を「店頭文書申請」しなければならなくなります。
しかし、一度だけそれ(ワンタイムパスの(Token ID の)再登録)をすれば、以降の本文書の手順に従うことで、複数の PC でワンタイムパスが使えるようになります。

「Set」ボタンで「Set ページ」に行き、「Backup」ボタンをおしてください。

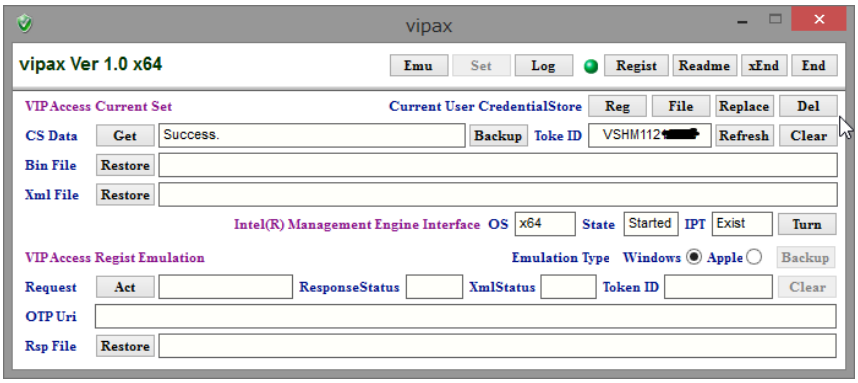


このような画面になりますので「OK」ボタンを押しバックアップを実行してください。

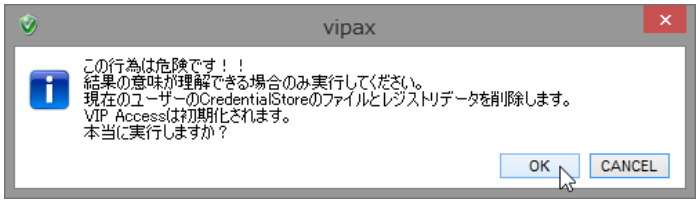
以下のような画面になりますので「OK」ボタンを押し進めてください。
基本的に実行ファイルディレクトリ直下の「backup」ディレクトリにデータは保存されます。
尚、既に保存済みのところを再度保存しようとすると(重複名ファイル)上書き実行確認のダイアログが出ます。



次に「Del」ボタンを押してください。

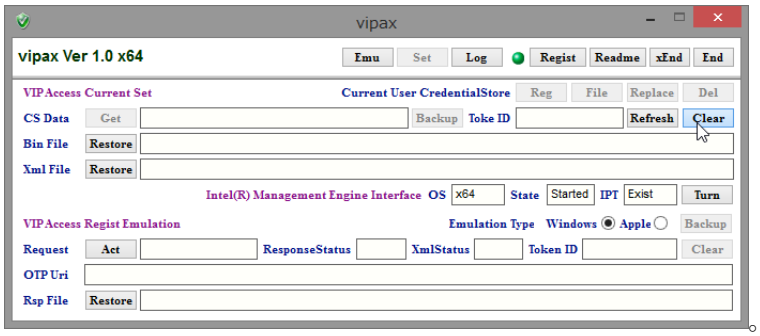


このような画面になりますので「OK」ボタンを押して先に進めてください。

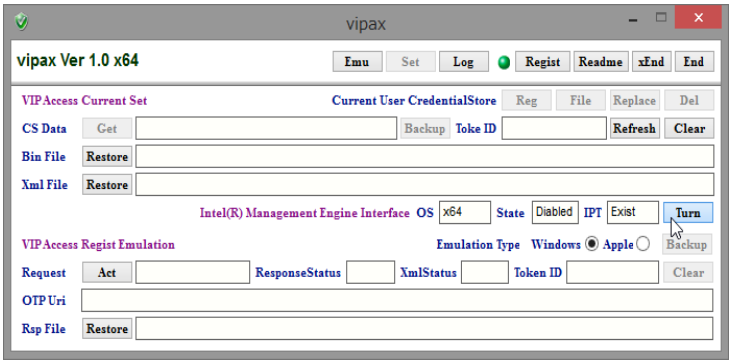


これで、現在の「VIP Access」の(CredentialStore)データは削除されます。

次に「Clear」ボタンを押して、現在本ソフトに読込まれているデータをクリアします。

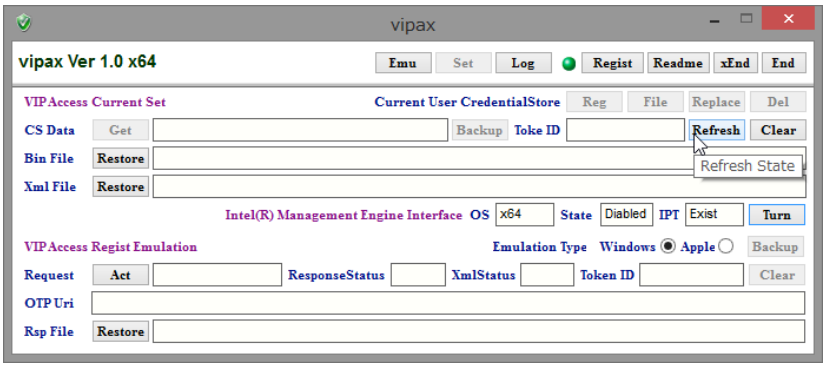


次に「Turn」ボタンを押して「Intel MEI」を無効化してください。
「State」が「Disabled」になっていることを確認してください。



ここで「VIP Access」を起動してください。
再度、Symatec サーバーに接続し「VIP Access」に新しい(CredentialStore)データが設定されます。
(「VIP Access を有効にしています」という画面が出てから「VIP Access」が起動します。)
ただ今度は「Intel IPT」が外れた状態でのデータが設定されるので、完全エミュレーションが可能です。
ここで「VIP Access」を終了してください。(しなくてもかまいません。)

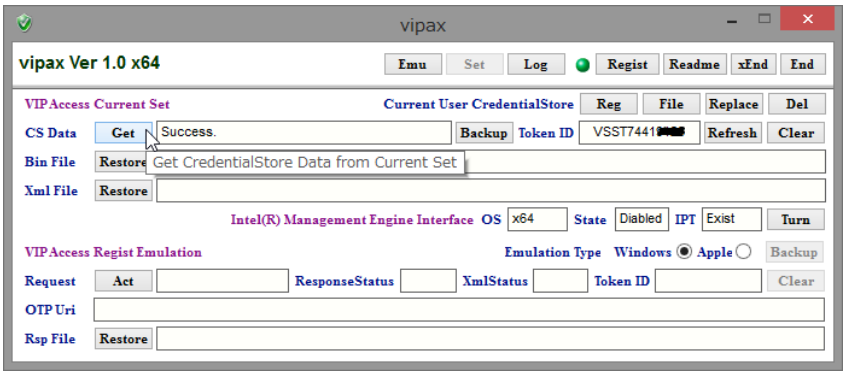
「Refresh」ボタンを押してください。



現在の状態が最新化して「Get」ボタンが有効化します。
ここで、以下の「Intel IPT」非稼働状態下での「VIP Access」稼働状態になります。

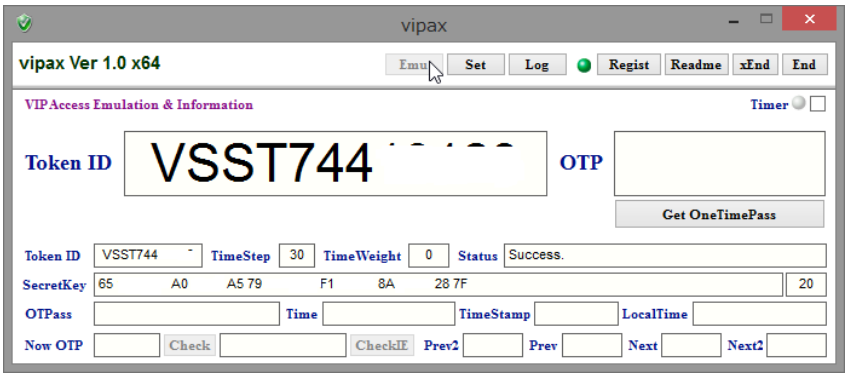
「INTEL IPT」が稼働していない状態で既に「VIP ASCCESS」を起動している場合

既に「VIP Access」を「Intel IPT」非稼働下の PC で起動している場合、次のような画面になります。
ここで、まだ「VIP Access」を導入していない場合は、そのインストールと初回実行を行ってください。
本ソフトを起動して「Set ページ」に入ると「Get」ボタンが有効化しているのでこれを押してください。



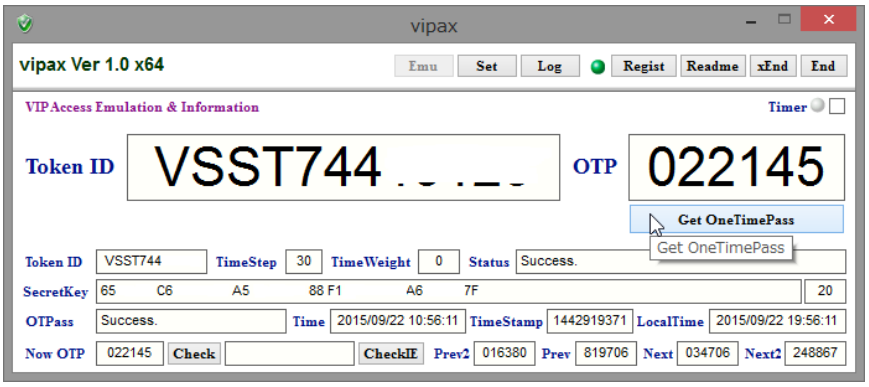
「Token ID」のプレフィックスが「VSHM」ではなく「VSST」であることを確認してください。
「VSHM」の場合は「Intel IPT」稼働下での「Token ID」となります。

「Emu」ボタンを押し「Emu ページ」に行ってください。



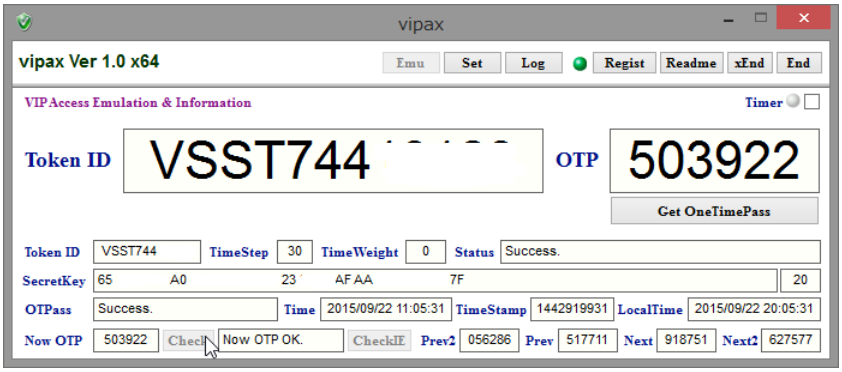
このような画面になるので「SecretKey」右端の「20」を確認してください。
これは「SecretKey」のバイト数ですが、これが「20」でない場合、処理が進められません。
「112」の場合は「Intel IPT」稼働下の状態ですので、上のその説明のところへ行ってください。

「Get OneTimePass」ボタンを押します。



このような画面になります。
ワンタイムパスとそれにまつわる各種情報が表示されます。

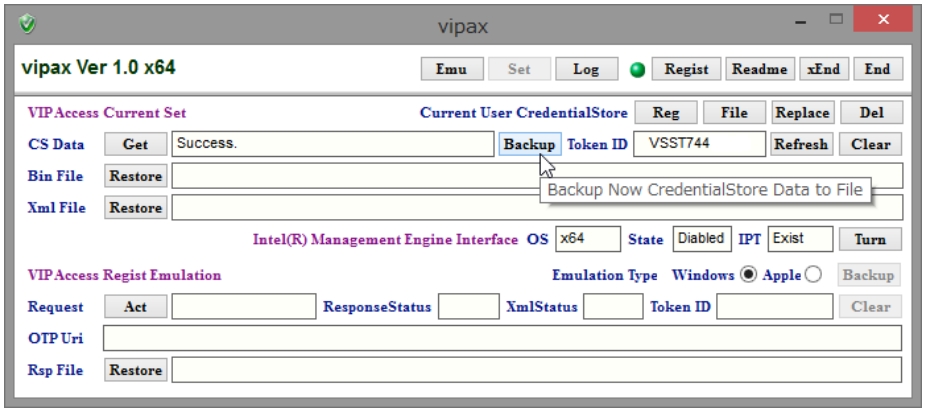
ここで「Check」ボタンを押してください。



Symantec サーバーに接続し「Now OTP」すなわち現在のワンタイムパスの正当性が検証されます。右側に「Now OTP OK.」と表示されれば OK です。時々エラーになるときがありますがそのときは再度「Check」検証、または 30 秒ほど待って再度「Get OneTimePass」ボタンを押して新しいワンタイムパスを取得してから「Check」検証してみてください。
何度やってもエラーになる場合は、なんらかのトラブルが発生しています。尚、一度検証通過したワンタイムパスを再度検証はできませんので、そのときは「Check」ボタンがグレーアウトします。30 秒ほど待って再度「Get OneTimePass」ボタンを押して新しいワンタイムパスを取得してください。それで「Check」ボタンは有効化します。

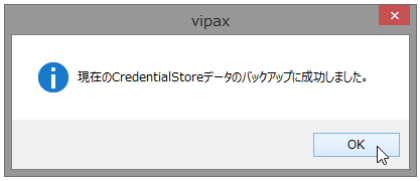
ネットバンキング等ではここでこの「VIP Access」の「Token ID」を登録してください。

そしてこの「VIP Access」のトークンを他の PC でも使えるようにバックアップします。
「Set」ボタンを押して「Set ページ」に行ってください。



「Backup」ボタンを押してください。
このような画面になりますので「OK」ボタンを押しバックアップを実行してください。

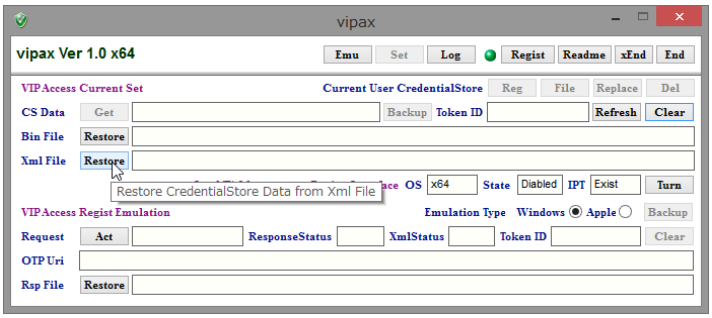
以下のような画面になりますので「OK」ボタンを押し進めてください。
基本的に実行ファイルディレクトリ直下の「backup」ディレクトリにデータは保存されます。
尚、既に保存済みのところを再度保存しようとすると(重複名ファイル)上書き実行確認のダイアログが出ます。



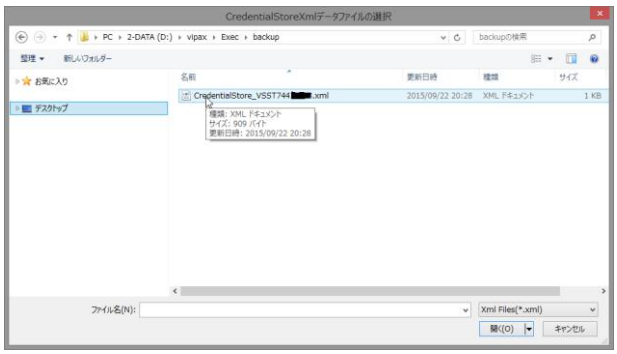
「INTEL IPT」が稼働していない状態でのバックアップデータの別 PC でのリストア

バックアップデータを他の PC でリストアして再現する方法を説明します。
本ソフトの実行ファイルが置かれたディレクトリを丸ごと別の PC の任意のディレクトリ上にコピーしてください
特に実行ファイルディレクトリ直下の backup ディレクトリ内のデータが無ければ意味がないことに注意ください。
別の PC では「VIP Access」をインストールすることも起動することも必要はありません。本ソフトがリストアデータから全て「VIP Access」をエミュレーションします。
そして「Intel IPT」の稼働、非稼働の問題も別の PC では関係ありません。

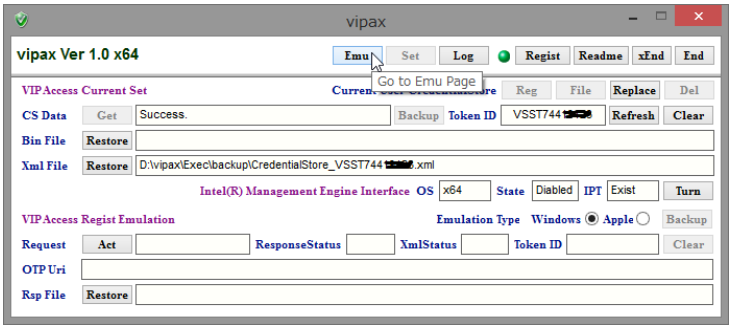
別の PC 上で本ソフトを起動し「Set ページ」に入って「Xml File」の「Restore」ボタンを押してください。



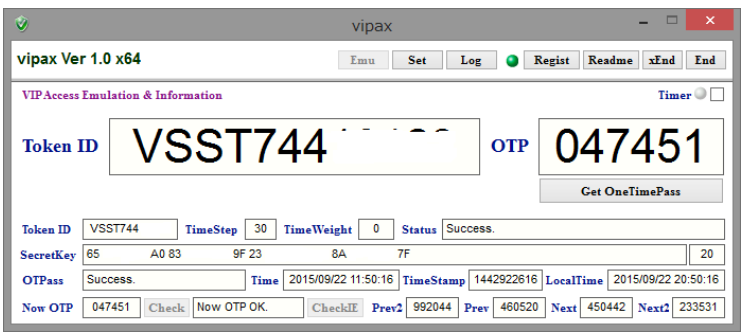
ファイル選択画面になり、先ほど保存したファイルが表示されるのでそれを選択し「開く」ボタンを押してください。



このような画面になるので「Emu」ボタンを押して「Emu パージ」に行ってください。



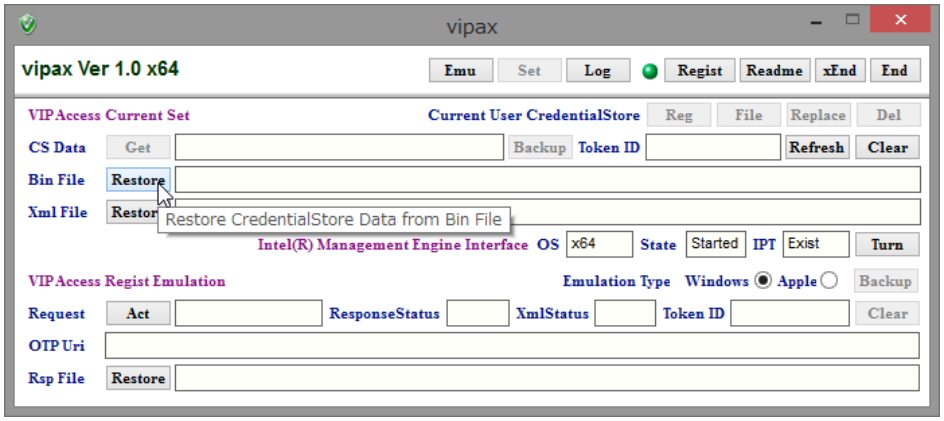
「Emu ページ」にて「Get OneTimePass」や「Check」ボタンを押して、正常にワンタイムパスが生成され、
かつその正当性が検証されることを確認してください。これでワンタイムパスの完全エミュレーションができました。



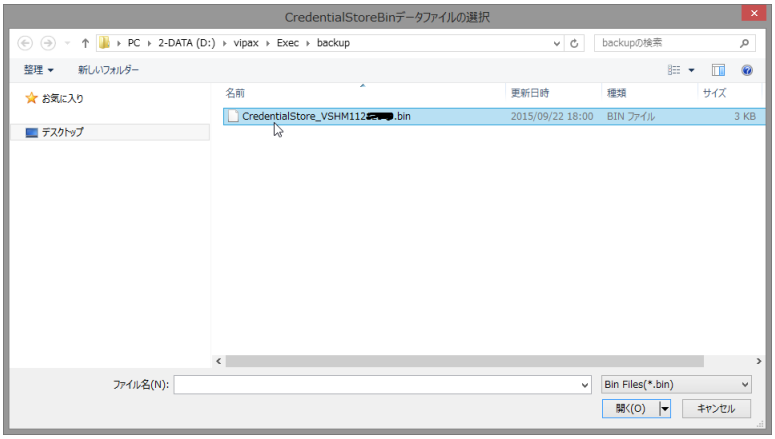
「INTEL IPT」が稼働している状態でのバックアップデータのリストアとリプレイス

先ほど「Intel ITP」が稼働している環境で、既に「VIP Access」を起動してしまった状態である場合に、そのバックアップデータを取りました。そしてその「VIP Access」の(CredentialStore)データを削除してしまいました。
そのバックアップデータのリストアとリプレイス方法を説明します。
ここで「リストア」とは、バックアップデータを本ソフトに読込み、ワンタイムパス生成をエミュレーションすること、いわば再現です。
これに対し「リプレイス」とは、バックアップデータを基に、「VIP Access」の(CredentialStore)データを再構築し、再度前の「VIP Access」状態を復元することになります。
「Intel IPT」稼働状態下でのバックアップした「VIP Access」の (CredentialStore)データは、そのバックアップしたPCでしか使えず、別のPC上で展開することはできません。

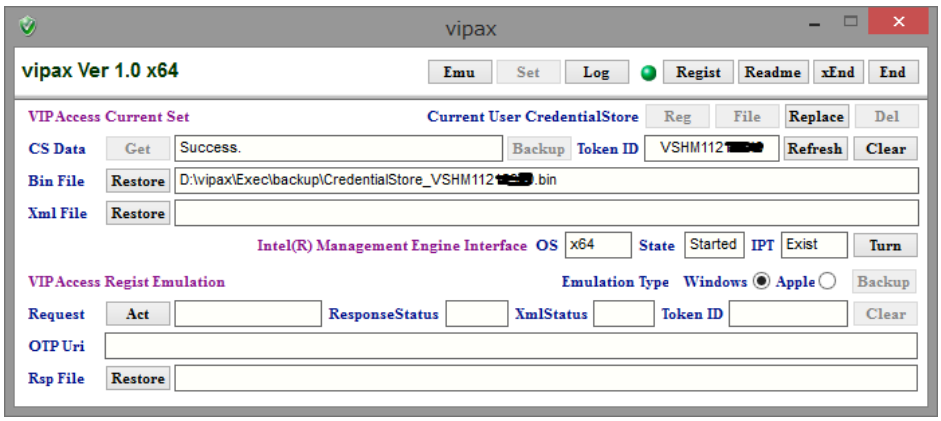
まず「Setページ」で「Intel MEI」を「Turn」ボタンで「Started」にし(そうなっていることを確認してください)
次に「Bin File」の「Restore」ボタンを押してください。



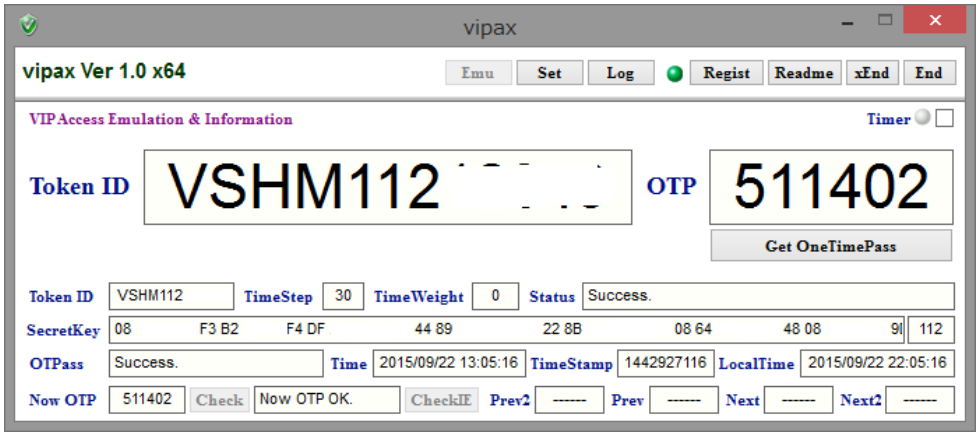
このような画面になるので、先ほど保存したファイルを選択し「開く」ボタンを押してください。



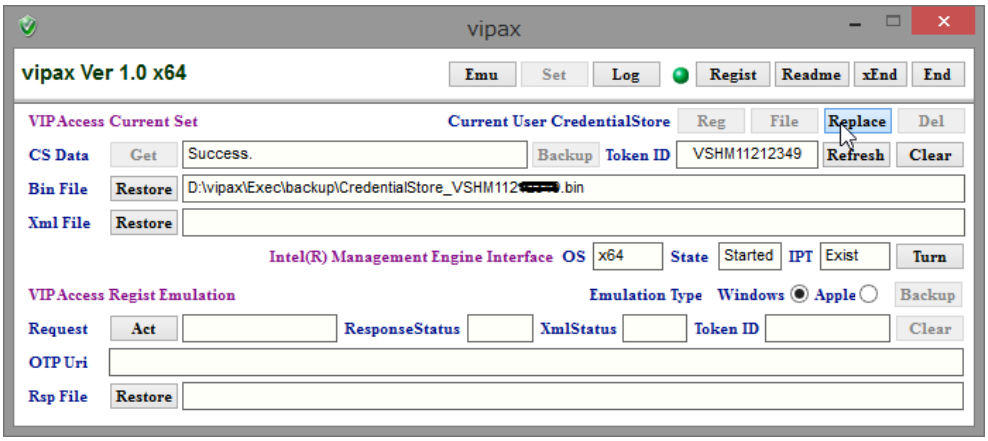
このような画面になります。



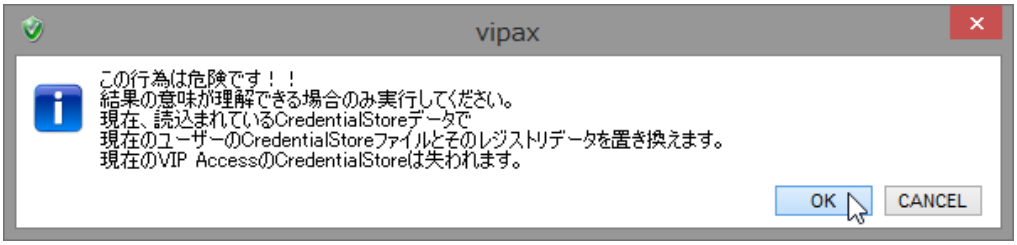
「Emu ページ」に行きワンタイムパス生成の検証を行ってみてください。



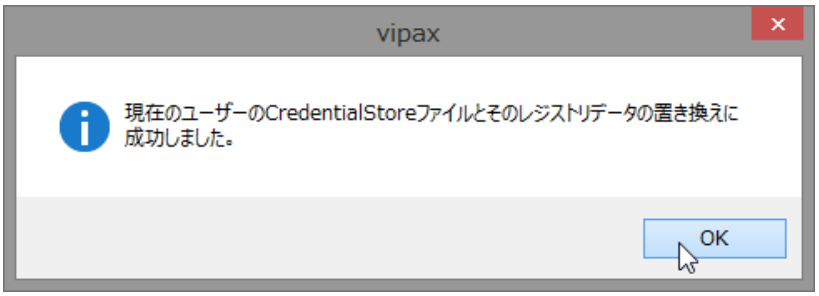
OK なことを確認してから「Set ページ」に戻り「Replace」ボタンを押します。



このような画面になるので「OK」で進みます。



このような画面になるので「OK」で完了します。



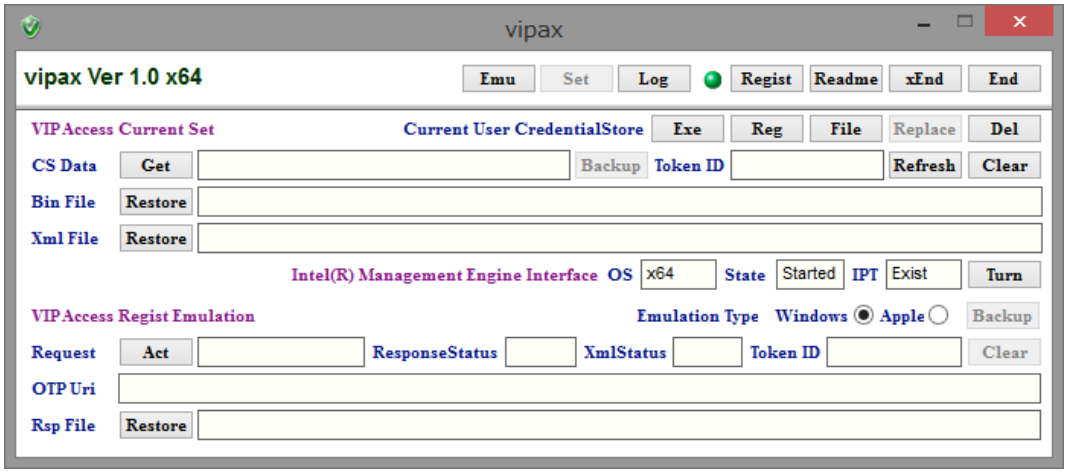
ここで「VIP Access」を起動してみてください。
「VIP Access」がリプレイスしたデータの「Token ID」で正常に動作していることを確認します。

各機能の説明

ここからは各ページでの機能の詳細を説明します。

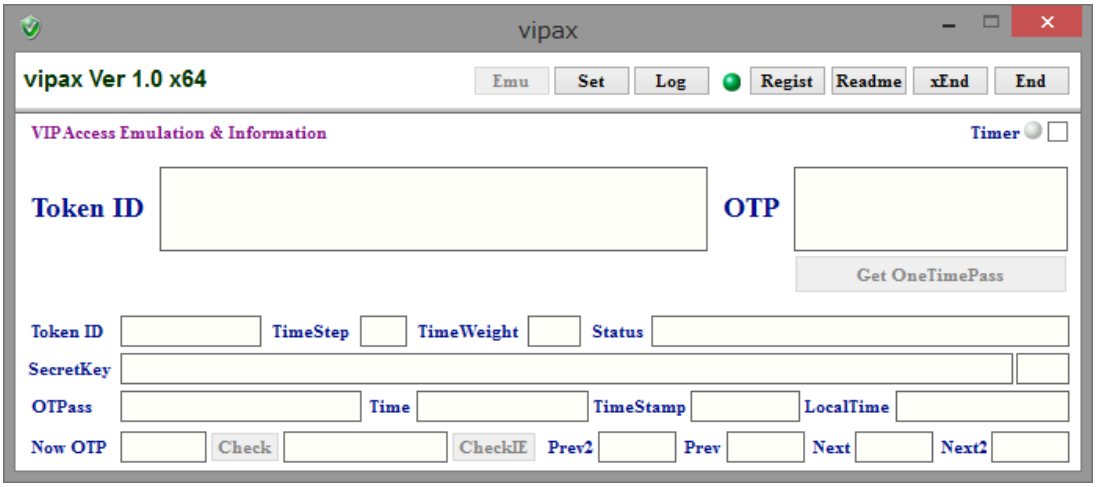
メインページの機能

画面上部のメインページは、ページを切り替えるための機能と本ソフトに共通する機能のある、どのページ行っても表示される固定画面です。



「Emu」「Set」「Log」ボタンは、各ページを切り替えます。
「Regist」ボタンは、購入登録画面を出します。
「Redme」ボタンは、本文書を表示します。
「xEnd」ボタンは、本ソフトを導入前の状態に初期化して終了します。
 原則として本ソフトがシステムに残したレジストリやファイルを全てを削除しますが、
 例外的に本ソフトの起動回数と使用日数の情報だけはシステムに残存させてもらっています。
「End」ボタンは、本ソフトを通常に終了します。尚、主だった設定は本ソフト再起動後も維持されます。

「EMU ページ」の機能



「Timer」チェックボックスは、
 それをオンにすると、自動で 10 秒ごとにワンタイムパスを取得するようになります。

「Token ID」は、「VIP Access」の「Token ID」を表示します。

「OTP」は、現在のワンタイムパスをを表示します。

「Get OneTimePass」ボタンは、ワンタイムパスを取得します。

「TimeStep」は、ワンタイムパスの更新間隔秒で通常「30」です。

「TimeWeight」は、ワンタイムパスを生成するとき、現在の時間にこの数字秒をマイナスしたものを
基礎時間とするもので、通常「0」ですが、プラスやマイナス数値があり得ます。

「Status」はワンタイムパス取得状況です。

「Time」はワンタイムパス生成の基礎時間です。

「TimeStamp」は基礎時間の Unix タイムスタンプです。

「LocalTime」は基礎時間のローカル時間です。

「Now OTP」は現在の

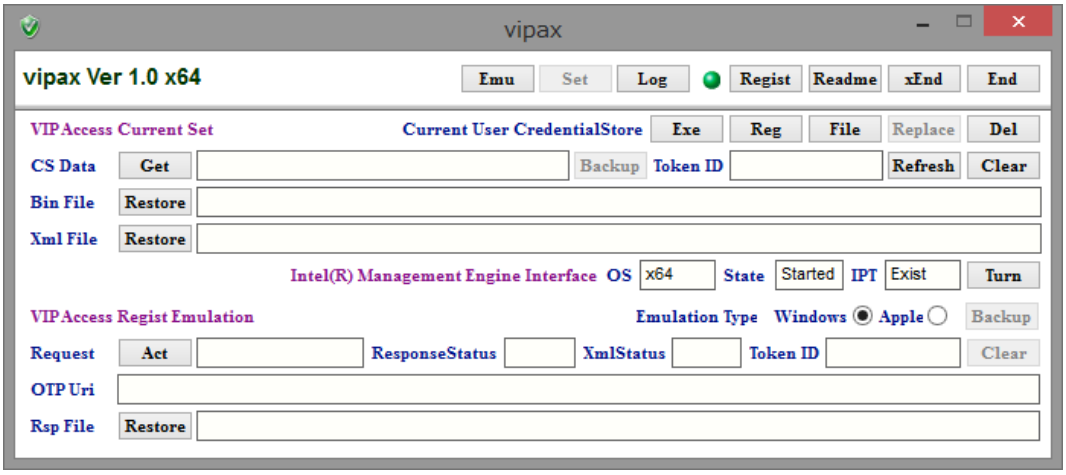
「Prev2」は前々回の、「Prev」は前回の、「Next」は次回の、「Next2」は次々回のワンタイムパスです。

「Check」ボタンは、Syamntec サーバーにて現在のワンタイムパスが正規か検証します。

「CheckIE」ボタンは、「Check」での検証を「InternetExplorer」上で行います。

「SET ページ」の「VIP ACCESS CURRENT SET」の機能

ここで、「Set ページ」の「VIP Access Current Set」各機能を説明します。



「Current User CredentialStore」の「Exe」ボタンは、「VIP Access」のクライアントソフトを起動します。

「Reg」ボタンは、
現在のユーザーの「VIP Access」の(CredentialStore)データのレジストリ保存をレジストリエディタで表示します。
「File」ボタンは、
現在のユーザーの「VIP Access」の(CredentialStore)データのファイル保存をエクスプローラで表示します。

「Replace」ボタンは、
現在本ソフトに読込まれているデータを基に、
現在のユーザーの「VIP Access」の(CredentialStore)データを再構築しそれをリプレイスします。
既存の現在のユーザーの「VIP Access」の(CredentialStore)データは破棄されますので注意が必要です。
通常この行為は、バックアップデータを本ソフトに読込み、それから行いますが、
「Intel ITP」が稼働していない環境でのバックアップデータは、「Intel ITP」が稼働していない環境で、
「Intel ITP」が稼働している環境でのバックアップデータは、「Intel ITP」が稼働してる環境でしか使えません。
また、「Intel ITP」が稼働している環境でのバックアップデータは、その PC でしか使えません。
リプレイス後、「VIP Access」を起動してその正常稼働を確認してください。
もしリプレイスがうまくいっていない場合は、「VIP Access」起動時に「VIP Access を有効にしています」
という画面が出て、データが再初期化されてしまいます。

「Del」ボタンは、
現在のユーザーの「VIP Access」の(CredentialStore)データを削除します。
「Reg」「File」ボタンの通り、「VIP Access」の(CredentialStore)データはレジストリとファイルに同一内容のものが保存されており、それを削除します。
これも既存の「VIP Access」の(CredentialStore)データは破棄されますので注意が必要です。
「Del」ボタンを押してから「VIP Access」を起動すると、必ず「VIP Access を有効にしています」という画面が出て、「VIP Access」によって(CredentialStore)データが再構築されます。

「Get」ボタンは、
本ソフトに、現在のユーザーの「VIP Access」の(CredentialStore)データを読込みます。
よって「VIP Access」の(CredentialStore)データがない場合(「VIP Access」を導入していないとか、そのデータを「Del」している場合)は使えません。

「Backup」ボタンは、
現在本ソフトに読み込まれている「VIP Access」の(CredentialStore)データをバックアップします。
バックアップ時は、データを再構築し「Bin File」と「Xml File」にして、
本ソフト実行ファイルディレクトリ直下の「backup」ディレクトリに、本ソフトが決定した名称で保存されます。
ファイル名の一部には「Token ID」が使われます。

「Refresh」ボタンは、本ソフトの「Set ページ」の現在の状態を更新表示します。

「Clear」ボタンは、
本ソフトに読込まれた、現在のユーザーの「VIP Access」の(CredentialStore)データをクリアします。
本ソフト上だけのことであり、「VIP Access」の(CredentialStore)データを削除するわけではありません。

「Bin File」の「Restore」ボタンは、
バックアップされた「Bin File」を基に、本ソフトに「VIP Access」の(CredentialStore)データを読込みます。

「Xml File」の「Restore」ボタンは、
バックアップされた「Xml File」を基に、本ソフトに「VIP Access」の(CredentialStore)データを読込みます。

バックアップデータをリストアする場合「Bin File」または「Xml File」からリストアします。
「Bin File」はMSの「Crypt(Un)ProtectData」APIによって暗号化されているため、原則として他のPCでは解読できませんが(姉妹ソフトの「pkfcr」を使えば解読できないことはないのですが)、
そもそもそれを解読したものが「Xml File」ですので、基本的に「Xml File」からリストアすれば問題ありません。
「Bin File」はそれをバックアップしたマシンでは解読できますので、その場合は「Bin File」からのリストアでもかまいません。本ソフトはバックアップ時に「Bin File」を現在のマシンで「CryptProtectData」し保存します。

「Intel(R) Management Engine Interface」の「OS」は、現在のPCのOSの状態(x86/x64/WOW64)を区別し表示します。

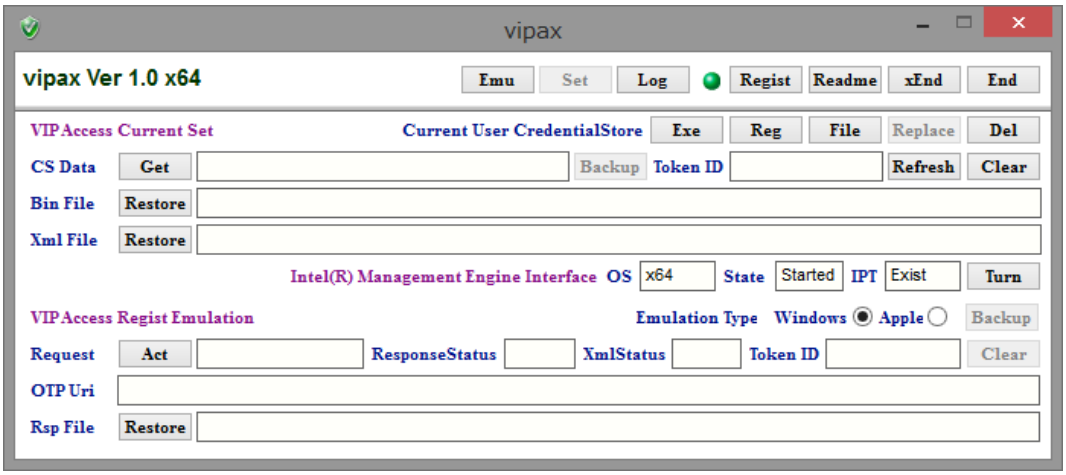
「State」は、「Intel MEI」の状態を表示します。

「IPT」は、「Intel IPT」の状態を表示します。
「Intel IPT」が存在し「Intel MEI」が稼働している場合、本ソフトは完全エミュレーションができません。

「Turn」ボタンは、「Intel MEI」をオンオフ(有効/無効化)します。

「SET ページ」の「VIP ACCESS REGIST EMULATION」の機能

ここで、「Set ページ」の「VIP Access Regist Emulation」各機能を説明します。



本機能は、「VIP Access」のクライアントソフト無しに、その「Token ID」の生成とその Symantec サーバーへの登録をエミュレーションします。このエミュレーションの結果取得されたレスポンスデータがあれば、「VIP Access」のクライアントソフト無しに、どの PC でもこの「Token ID」での「VIP Access」エミュレーションが可能です。

「Emulation Type」は「Windows」と「Apple」タイプが選択できます。
内部的に一定のパラメタで本エミュレーションが行われますが、
「Apple」タイプの場合、こちらマシンは「MacBookPro12.4」として振る舞い
Symantec サーバーと 1 回の通信で登録が完了します。。
通常は「Windows」タイプで行います。
この場合「ActivationCode」取得のため、Symantec サーバーとは 2 回の通信となり完了します。

「Backup」ボタンは、Symantec サーバーからのレスポンス内容を保存します。
バックアップデータ(Rsp File)は Xml 型のファイルで拡張子は「.rsp」となります。
このバックアップデータを使うことで、
どのマシンでもその「Token ID」でのワンタイムパス生成エミュレーションが可能です。

「Act」ボタンは、本エミュレーションの実行を開始します。

「ResponseStatus」は、
本エミュレーションで、Symantec サーバーからのレスポンス獲得に成功したか否かを表示します。
「XmlStatus」は、
Symantec サーバーからのレスポンスを解読して Xml(バックアップデータ)化に成功したか否かを表示します。

「Token ID」は、本エミュレーションで生成された「Token ID」を表し、ユーザーが任意に決めることはできません。

「Clear」ボタンは、本エミュレーションで取得したデータをクリアします。
「Clear」する前に適宜「Backup」しておく必要があります。

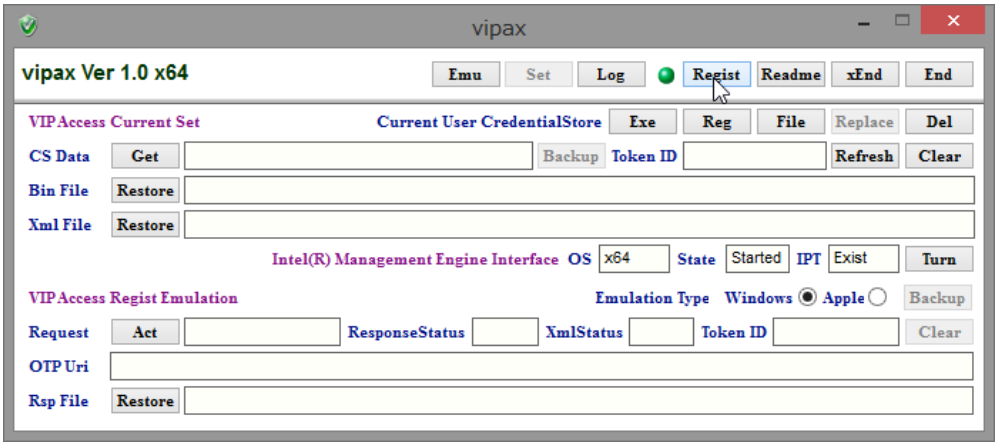
「Rsp File」の「Restore」ボタンは、本エミュレーションのバックアップデータをリストアして、
本ソフト内に「VIP Access」の(CredentialStore)データを構築します。
リストア後は「Emu ページ」にてワンタイムパス生成が可能になります。

「LOGT ページ」の機能

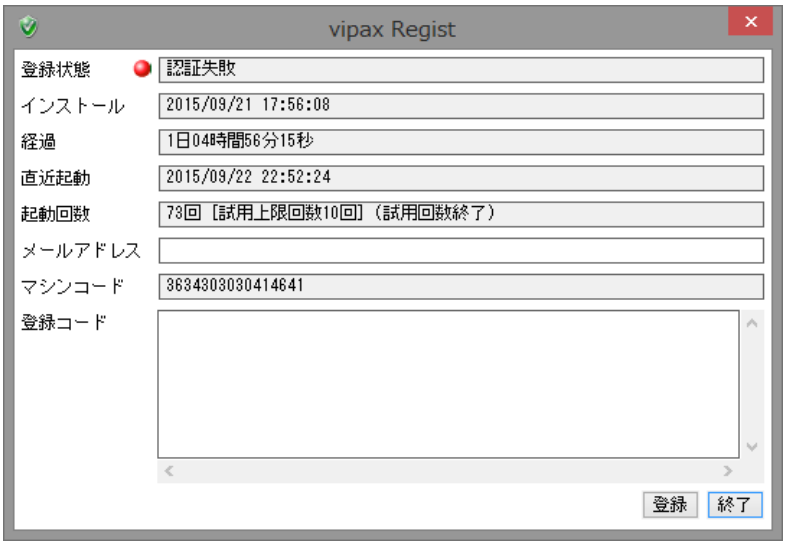
各種アクションで本ソフトは自動でログを取ります。そのログを表示するページです。
ユーザーはその内容に関知する必要はありません。
「Clear」ボタンは、ログ画面の内容をクリアします。

(購入)登録方法

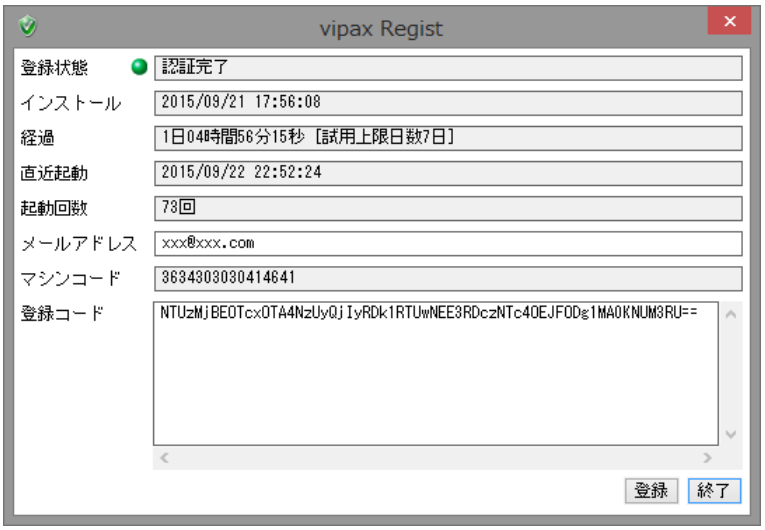
登録方法を説明します。画面上部の「Regist」ボタンを押します。



このような画面になるので、登録した「メールアドレス」と、送られた「登録コード」を入力します。



「マシンコード」はここでは関係ないので無視してください。
「インストール」日時、「直近起動」日時、「起動回数」は継続的に記録されていきます。
「登録」ボタンを押します。正しい「登録コード」が入力されていれば「認証完了」となります。



登録後は画面上方のマークが上図のとおり緑色になります。
このマークは試用中は黄色、試用期間回数切れの場合は赤色、登録時は緑色になります。